Skadden

Privacy & Cybersecurity Update

Pennsylvania Supreme Court Recognizes Common Law Duty to Protect Employee Personal Data

The Supreme Court of Pennsylvania has ruled that employers have a common law duty to protect data against unauthorized access. This decision could signal a dramatic expansion of data protection rights in the United States beyond contract-based requirements.

On November 21, 2018, the Supreme Court of Pennsylvania decided in *Dittman v. UPMC*,[1] ruling that employers have a common law duty to use reasonable care to safeguard their employees' sensitive personal information on an internet-accessible computer. As a result, employees may bring a general negligence claim against their employer on an independent basis from any rights they may have under their employment agreement, including in the case of a data breach.

Background

In 2014, the University of Pittsburgh Medical Center (UPMC) suffered a data breach involving the sensitive personal information of 62,000 current and former employees that included names, birth dates, Social Security numbers, addresses, tax information, bank account information and salary information. Employees were required to provide this information as a condition of employment at UPMC. After the breach, third parties fraudulently used the information to file fraudulent tax returns on behalf of the victims, resulting in alleged actual damages for the impacted employees. The plaintiffs also alleged the breach would put them at "increased and imminent risk" of being further victimized by fraud in the future.

Impacted employees filed a class action claim against UPMC, alleging breach of implied contract and negligence.[2] The trial court dismissed the negligence claim, holding that Pennsylvania's economic loss doctrine precluded the action because the plaintiffs asserted solely economic losses. The court reasoned that prior appellate rulings decidedly blocked such a recovery under a negligence cause of action. Notwithstanding this basis, the trial court also declined to impose a new affirmative duty of care to protect data. The court noted the frequency and magnitude of modern data breaches

[1] The decision is available online here.

[2] The employees' breach of contract claim also was dismissed and not at issue in this appeal.

and determined the resulting lawsuits against businesses would overwhelm the judicial system. Additionally, the trial court found no generally accepted standard of care for protecting one's data, meaning that when combined with the potential liability for businesses, the balance of social equities didn't clearly favor such a duty. Finally, the trial court identified related state legislative activity on data security issues and remarked that the legislature is best situated to define the modern standard of general security duties. The appellate court affirmed the decision of the trial court.

Decision

The Supreme Court of Pennsylvania reversed the decision of the lower courts and held that:

- UPMC had a legal duty of reasonable care to protect the sensitive employee information stored on an internet-accessible computer; and
- Pennsylvania's "economic loss" doctrine did not prevent the plaintiffs from asserting a negligence claim independent of their employment contract.

In its first finding, the court explained that it was not creating a new employer duty, but simply applying an existing duty of reasonable care under the circumstances to a novel factual scenario. In the case of employee information, general duty of care includes a duty to take reasonable measures to protect sensitive employee information against the foreseeable risk of a data breach.

In its second finding, the court reasoned that a plaintiff is not barred from recovering economic losses simply because the action arises out of tort law rather than contract law. Traditionally, the economic loss doctrine precludes a negligence tort claim where the plaintiff's cause of action is simply for breach of contract. However, the court found in this case that, since UPMC owed an independent duty to the employees apart from any contract between the parties, the economic loss doctrine was not a bar to their negligence cause of action.

Notably, the court's language on the economic loss doctrine issue is broad enough to suggest the same rationale could apply to a breach of customer data. For example, a company may owe data subjects a duty of care with respect to their personal information that exists independently and alongside their contractual and/or privacy policy commitments.

Expansion of Traditional Privacy Laws

This decision could be the beginning of a dramatic expansion of data breach protections for data subjects in the United States. Traditionally, data holders had to address two general compliance regimes:

- those imposed by federal statutes and regulations (such as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Children's Online Protection Act and, somewhat more generally, the Federal Trade Commission Act's general prohibition on unfair or deceptive trade practices), or by a patchwork of state statutes (such as the California Consumer Privacy Act); and
- contractual obligations, whether expressed through the data holder's own privacy policies or contractual commitments with third parties.

The *Dittman* decision suggests that, in addition to these more specific obligations, employers and possibly other data holders also owe a general duty of care to the individuals for whom they hold personal information. Whether Pennsylvania's or other courts will extend this obligation beyond employers — who already have a close relation with their employees — remains to be seen.

Key Takeaways

Pennsylvania employers now have a heightened common law responsibility to protect employee information based on foreseeable risks to their IT systems. Though *Dittman* was a Pennsylvania case, it may serve as a blueprint for courts in other states to re-evaluate employer responsibility given modern cybersecurity risks. Indeed, Pennsylvania and other state and local courts may expand this concept beyond employer-employee relationships and apply it in other areas, such as customer relationships, or even to areas such as data brokering where the data holder may have no other relationship with the data subject.

When evaluating their data security practices and potential liability in the event of a data breach, processors of personal data should not assume those duties are limited to statutory or contractual boundaries and should consider claims asserting a more general duty of care with respect to this information.

Return to Table of Contents

New HHS Guidelines May Help Define 'Reasonable' Security Standards

The U.S. Department of Health and Human Services (HHS) released a set of cybersecurity best practices for health care organizations. These guidelines may unofficially set the standard for "reasonable" cybersecurity in the industry and influence data security-related litigation under state and federal law.

New HHS Guidelines

On December 28, 2018, the U.S. Department of Health and Human Services published a voluntary set of guidelines titled "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients."[3] HHS developed the guidelines in accordance with the Cybersecurity Act of 2015 (CSA), which required the secretary of HHS to establish a set of voluntary, industry-led guidelines and best practices that would serve as a resource for reducing cybersecurity risks and support voluntary implementation of safeguards against common cybersecurity threats.[4]

The guidelines identify and describe five key cybersecurity threats in the health care industry:

- **Email phishing attacks:** Phishing is a common cybersecurity threat across many industries and occurs when an attacker sends an email that appears to come from a legitimate source, such as a coworker or manager. The attacker attempts to trick the recipient into sharing information or granting access to the organization's systems or data.
- **Ransomware attacks:** Ransomware is a specific type of malware that encrypts user data until the user or organization pays a ransom. A ransomware attack severely impacted the United Kingdom's National Health Service in 2017.
- **Loss or theft of equipment or data:** HHS described several risks that lead to loss or theft of equipment or data, including use of unencrypted devices and inadequate physical security practices in health care organizations.
- **Insider, accidental or intentional data loss:** HHS distinguished between intentional threats raised by insiders (*e.g.*, an employee who views and shares protected health information for inappropriate and illegal reasons) and unintentional threats, including inadvertent data loss or disclosure as a result of procedural errors.
- **Attacks against connected medical devices that may affect patient safety:** HHS highlighted several issues related to connected medical devices, such as potential security vulnerabilities in heart monitors connected to a hospital's computer network.

The publication described best practices to address these threats, with HHS dividing these best practices into the following general categories:

- email protection systems;
- endpoint protection systems;
- access management;
- data protection and loss prevention;
- asset management;
- network management;
- vulnerability management;
- incident response;
- medical device security; and
- cybersecurity policies.

For each category, HHS provided best practices for small, medium and large organizations. The end result is a set of guidelines that health care organizations of all sizes can use to address key cybersecurity risks and assess their current cybersecurity-related policies and protections.

Setting the Standard for 'Reasonable' Security Practices

The HHS publication does not require organizations to abide by any specific set of practices. However, many organizations — and perhaps more importantly, private litigants and judges — may view the publication's guidelines as a baseline for "reasonable" data security practices. Litigants who rely on state law theories of negligence or on broad contractual obligations to maintain reasonable security practices may argue that health care organizations that fail to follow the HHS guidelines also fail to meet their duties and obligations to patients and business partners. Similarly, the Federal Trade Commission (FTC) could assert that a health care organization's failure to abide by the HHS guidelines constitutes an unfair data security practice in violation of Section 5 of the FTC Act, which grants the FTC the authority to challenge such data security practices based in part on the reasonableness of those practices. Alternatively, if a company's privacy policy or other statements to consumers promise a "reasonable" security program, the FTC could use

[3] The first volume of the HHS publication is available here.

[4] The full text of the Cybersecurity Act of 2015 is available here.

the HHS guidelines to inform its assessment of whether the company has met that standard and, if it hasn't, accuse the company of deceptive business practices under the FTC Act.

As a result, although the guidelines likely will prove useful to many health care organizations as they prepare against cybersecurity threats, they also may incidentally create a de facto standard of care and thereby increase litigation involving allegations of unreasonable data security practices.

Key Takeaways

Health care organizations carefully should review HHS's guidelines and assess their own cybersecurity standards against those guidelines. Although the guidelines are voluntary, they may effectively set the standard for reasonable cybersecurity practices in the industry.

Return to Table of Contents

Vermont Supreme Court Holds That 'False Pretense' Exclusion Does Not Bar Coverage for Phishing Scam Loss

The Vermont Supreme Court recently held that a "False Pretense" exclusion in a business-owner insurance policy did not preclude the insured, from seeking coverage for monetary loss resulting from a phishing scam.

On December 28, 2018, the Vermont Supreme Court held, as a matter of first impression, that a False Pretense exclusion in Rainforest's business-owner insurance policy issued by Sentinel Insurance Company (Sentinel) did not exclude coverage for Rainforest Chocolate, LLC's (Rainforest) monetary loss resulting from a phishing scam.[5] The court reasoned that the False Pretense exclusion was ambiguous and therefore must be construed in favor of Rainforest as the policyholder.

Phishing Scam Loss and Denial of Coverage

In May 2016, a Rainforest employee received an email from his manager's email address, directing the employee to wire $19,875 to an outside bank account. The employee electronically transferred the money, not knowing that the email was actually sent by a fraudster who had gained unauthorized control of the manager's email account. After discovering the fraud, Rainforest contacted its bank, which was able to limit the loss to $10,261.36.

Rainforest reported the loss to Sentinel, claiming that the fraudulent wire transfer was covered under several policy provisions, including the Forgery, Theft of Money and Securities and Computer Fraud provisions. Sentinel denied coverage, primarily in reliance on the False Pretense exclusion in the policy, which excludes coverage "for physical loss or physical damage caused by or resulting from … [v]oluntarily parting with any property by you or anyone else to whom you have entrusted the property if induced to do so by any fraudulent scheme, trick, device or false pretense."

Coverage Litigation

The trial court granted summary judgment for Sentinel, reasoning that the False Pretense exclusion unambiguously barred coverage for Rainforest's money loss, which Rainforest appealed. On appeal, Rainforest argued that the False Pretense exclusion was inapplicable because the exclusion only bars coverage for "*physical* loss or physical damages" and the loss at issue — a fraudulent transfer of money via electronic means — was not a physical loss. Sentinel countered that the exclusion applied because Rainforest lost "physical control and possession" of the money.

The Vermont Supreme Court reversed, holding that "the loss suffered was not physical, and thus coverage is not barred by the False Pretense exclusion." The court reasoned that because the False Pretense exclusion was subject to at least two reasonable interpretations as to whether the loss of electronic funds constituted a "physical loss," the False Pretense exclusion was ambiguous. It therefore construed the exclusion against Sentinel and remanded the case for consideration of whether the loss falls within one of the policy's coverage grants in the first instance.

In concluding that the False Pretense exclusion was ambiguous, the court relied heavily on a Montana federal court case, *Ad Advertising Design, Inc. v. Sentinel Insurance Co., Ltd.*,[6] which found identical policy language to be ambiguous in an analogous factual scenario because courts have interpreted the same or similar language in differing but reasonable manners. For example, some courts have concluded that the loss of money via a fraudulent wire transfer constitutes a "physical loss" because intangible funds are interchangeable with tangible money; whereas other courts have concluded that funds deposited into

[5] *Rainforest Chocolate, LLC v. Sentinel Ins. Co., Ltd.*, No. 2018-095, 2018 WL 6817065 (Vt. Dec. 28, 2018).

[6] 344 F. Supp. 3d 1175 (D. Mont. 2018).

a bank account do not have a "physical" existence and therefore are not susceptible to physical loss or damage. The court also pointed to the fact that the policy uses the phrase "physical loss and physical damage" and the phrase "loss and damage," which suggests that Sentinel, in drafting the policy, contemplated that not all losses of money were physical in nature.

Key Takeaways

Although the *Rainforest Chocolate* decision involved a relatively small amount of money, it serves as a cautionary tale for both insurers and policyholders. The Vermont Supreme Court held that Rainforest was not precluded from pursuing coverage for its cyber-related loss under a non-cyber specific business-owner insurance policy. However, it just as easily could have reached the opposite conclusion, as other courts have. Insurers and policyholders carefully should review their policies to make the parties' intentions with respect to coverage clear. In particular, insurers should avoid or define inconsistent terms and phrases to fend off allegations that their policies are ambiguous.

Return to Table of Contents

2018 Survey Reveals Continued Evolution and Expansion of Cyber Insurance Market and Other Recent Trends

Reinsurer PartnerRe recently published a report that highlights cyber insurance market trends of 2018.

A recent report published by PartnerRe, which is based on a survey of 2018 cyber insurance market trends conducted for the fifth year in a row in conjunction with Advisen, reveals that the cyber insurance market continued to grow and mature in 2018, while also highlighting key marketplace trends.[7] The survey respondents were brokers and underwriters primarily from North America, as were most of their insureds.

According to the report, one recent trend is that small and midsize businesses took center stage among the new-to-market buyers of cyber insurance. The survey showed that 44 percent of new buyers were small companies (revenues of less than $50 million) and 45 percent were midsize companies (revenues of $50 million to $1 billion). The report opines that these numbers are "an indication that smaller businesses are beginning to more fully understand their [cyber] risks."

In addition to the increase in cyber insurance purchases by small and midsize businesses, the survey reports a healthy increase in cyber insurance take-up by less traditional industries, such as manufacturing. In the end, however, the survey shows that the health care industry brought in the most new-to-market buyers of cyber insurance (42 percent), followed by manufacturing (40 percent), professional services (38 percent), financial services (38 percent), information technology (38 percent), retail (24 percent), government/nonprofit (18 percent), energy (18 percent), education (16 percent) and other (8 percent). According to the survey, the two main drivers for businesses purchasing cyber insurance were learning of cyber incidents in the media and the possibility of suffering a cyber incident, as was the case in prior years.

The primary obstacle to cyber insurance sales continues to be a lack of understanding about risk exposure, with 75 percent of respondents reporting that their clients simply do not understand their cyber risk exposures. Other obstacles identified by respondents include clients not understanding coverage (56 percent), cost (42 percent), the application process (35 percent), and varying policy forms and coverages (26 percent).

Another 2018 trend, according to the report, is increased competition in the cyber insurance market. Respondents almost unanimously (90 percent) said that competition had increased from 2017, largely due to new insurers joining the marketplace in 2018. In addition, the report indicates that both cyber insurance pricing and wording have become more consistent. An overwhelming 90 percent of respondents said that cyber coverage expansion is necessary to stay competitive in the current cyber insurance market, which the report interprets as a signal "that carriers who do not provide coverage that is at least in line with what is offered by most will be at a competitive disadvantage." However, considerable variation among policy forms caused 67 percent of respondents to report working with only a few carriers to avoid having to deal with varying coverages and wording.

The report also indicates that the 2017 trend toward standalone cyber policies continued in 2018. Respondents identified the need for dedicated cyber limits and expanded business interruption coverage as the top two reasons for switching from cyber insurance endorsements on non-cyber policies to standalone cyber policies. However, when asked to identify the coverage lines for which they most frequently write cyber endorsements, respondents reported that errors and omissions coverage was the most commonly endorsed coverage line (72 percent), followed by directors and officers liability/employment practices liability (58 percent) and crime (57 percent).

[7] The "2018 Survey of Cyber Insurance Market Trends" can be found here.

Key Takeaways

As the report indicates, businesses of all sizes and across diverse industries increasingly are turning to cyber insurance as one component of their risk management plans, with insurers continuing to improve their cyber insurance products in order to remain competitive in this space and complement their other offerings. In light of the ever-growing frequency and severity of cyberattacks and losses in the interconnected world, we expect the cyber insurance market to continue to grow and evolve in 2019.

Return to Table of Contents

Neiman Marcus Settles with Attorneys General Over Multistate Data Breach

Neiman Marcus has settled state claims arising out of a 2013 data breach that impacted customers in many U.S. states. The settlement requires the retail chain to pay $1.5 million to various states and implement a number of security measures.

On January 7, 2019, Neiman Marcus Group LLC (Neiman Marcus) settled with 43 states and the District of Columbia to resolve an investigation into a 2013 data breach that affected thousands of Neiman Marcus customers. The upscale department store agreed to pay the states an aggregate amount of $1.5 million and implement a variety of cybersecurity measures to reduce the risk of a similar attack in the future.

In January 2014, Neiman Marcus disclosed that its customers' credit card information had been compromised. Malicious hackers surreptitiously installed software on its systems that copied the information. State attorneys general launched an investigation, led by Illinois Attorney General Lisa Madigan and Connecticut Attorney General George Jepsen. The investigation found that the credit card information of more than 370,000 credit cards used at 77 stores had been compromised. At least 9,200 of the cards were later used for fraudulent purposes.

The settlement payment will be divided among the participating states and used for a variety of purposes as determined by the respective attorneys general. Some of the payments, for example, will likely be placed into a consumer protection law enforcement fund or used to cover the costs of the investigation. None of the payments are specifically earmarked to provide compensation to affected consumers.

In addition to the payment, the settlement requires Neiman Marcus to take a number of steps to improve its information security, many of which are — or should be — ordinary course practices for any company handling payment card information. These steps include:

- complying with the Payment Card Industry (PCI) Data Security Standard and having agreements in place with two separate PCI forensic investigators;
- putting in place a system to collect and monitor network activity, and regularly reviewing activity logs;
- updating the software it uses to maintain and safeguard personal information, and creating written plans for addressing software that is reaching its end-of-life or end-of-support date;
- implementing steps to review industry-accepted payment security technologies relevant to its business; and
- implementing measures to reduce the value of the payment card information it holds, such as using encryption and tokenization technologies.

The company also will have an ongoing dialogue with the attorney general of Connecticut, as the settlement requires Neiman Marcus to obtain and submit to the attorney general's office an information security report from a third-party assessor verifying it has put the required security measures in place. It also must provide the attorney general with a Response Report describing any further actions it plans to take as a result of any deficiencies noted in the third-party assessor's evaluation. The attorney general will then work with Neiman Marcus as the company seeks to address those deficiencies.

Pursuant to the terms of the settlement agreement, all of the attorneys general agreed not to pursue any civil claims against Neiman Marcus in connection with the breach. Consumer claims are not affected by the settlement and, in fact, the company still faces a federal class action lawsuit related to the breach.

Key Takeaways

The Neiman Marcus data breach and settlement signify the need for companies to ensure their information security to safeguard against potential cyberattacks. The steps the company is being forced to take as part of the settlement agreement would be good practice for any company to follow.

Return to Table of Contents

California Attorney General Hosts First Public Hearing on California Consumer Privacy Act

The California Attorney General's Office hosted the first of seven public hearings to solicit comments on the California Consumer Protection Act. However, major uncertainties regarding the scope and requirements of the law continue to challenge early compliance efforts by impacted businesses.

On January 8, 2019, representatives from the California Attorney General's Office hosted a public hearing in San Francisco to receive public feedback on the California Consumer Privacy Act (CCPA). Under Section 1798.185 of the CCPA, the California attorney general is directed to encourage public feedback and develop new regulations to further the goals of the CCPA. Specifically, prior to enforcement, the attorney general's office must develop regulations in a number of enumerated areas, including consumer opt-out procedures, a uniform opt-out button, accessibility requirements and verified consumer request processing requirements.

Background

On June 28, 2018, Gov. Jerry Brown signed the CCPA into law, which was followed by an amendment to the CCPA signed into practice on September 23, 2018, which delayed enforcement of the law and provided several clarifications.[8]

The primary goal of the CCPA is to give consumers greater visibility and control over how their data is collected, used and shared by businesses covered by the law. Upon consumer request, businesses must delete data provided by the consumer, respect a request not to sell or share personal information with third parties, and provide background information on the personal information possessed by the business and how they share such data. Additionally, businesses must publicize these practices through a privacy policy or on their website.

Key Speaker Concerns

While only around a dozen speakers provided input out of an audience of hundreds, there were several repeating themes expressed in the public comments:

- **Definition of Personal Information:** The current language of the CCPA covers an expansive data set and includes some types of personal information not expressly covered by other data protection regimes, such as the European Union's General Data Protection Regulation (GDPR). Nearly every speaker requested that the attorney general provide greater clarification by narrowing the definition.
- **Unintentional Increase in Data Collection Requirements:** In order for a consumer to initiate a consumer information request, the requestor must provide a verifiable consumer request form. The CCPA gives a limited explanation of the form required, and the attorney general is charged with providing greater specificity. Many businesses set to come under the purview of the requirement worry that the amount of information needed to verify a consumer request would be more than they ordinarily would collect. Ironically, the businesses would have to collect more information from the consumer for the sole purpose of verifying any later information requests. As a result, many speakers urged the attorney general to carefully develop verification obligations to avoid undermining data minimization efforts.
- **Streamlining with GDPR Requirements Where Possible:** Several industry speakers noted the expensive and complex operational steps recently undertaken by many businesses to comply with GDPR requirements. They asked the attorney general to standardize CCPA and GDPR obligations, where possible, and to take advantage of existing infrastructure and business processes while also minimizing unique compliance costs.

Key Takeaways

The rapid passage of the CCPA and delegation of certain implementation decisions to the attorney general means businesses must remain nimble and attentive as regulations are clarified in the coming months. The lack of guidance thus far from the attorney general is inhibiting early compliance preparation, but presents an opportunity for businesses to submit feedback during the public comment period and potentially influence the ultimate regulations.

Return to Table of Contents

[8] We previously discussed the CCPA in a July 2018 client alert that can be found here and discussed amendments to the CCPA in our September 2018 *Privacy & Cybersecurity Update*, which can be found here.

EU Announces Adequacy Decision for Japan's Data Protection Regulations

The European Union and Japan have issued mutual adequacy decisions, enabling personal information to flow between the two regions.

On January 22 and 23, 2019, Japan and the European Commission (EC) each adopted adequacy decisions allowing personal data to flow freely between the EU and Japan. The decision was the final step in a process[9] launched in September 2018, in which Japan endeavored to comply with stricter European data regulations under the GDPR.

Background

Under the GDPR, EU personal data only may be transferred outside the EU if the recipient country has achieved "essential equivalence" with EU data protection regulations and the European Commission has issued an adequacy decision. The mutual adequacy decisions between the EU and Japan come in the midst of trade negotiations and will complement the EU-Japan Economic Partnership Agreement, which goes into effect in February 2019. The Economic Partnership Agreement will facilitate trade between the two economic regions by removing tariffs and opening markets. In its press release regarding the adequacy decision, the European Commission affirmed that "in the digital era, promoting high privacy and personal data protection standards and facilitating international trade must and can go hand in hand."

This is the first EC adequacy decision since the GDPR came into full legal effect. The EC previously has adopted adequacy decisions for 12 other countries under the region's prior data privacy law, where such decisions remain in effect. These additional decisions include, for example, a decision relating to the U.S. Privacy Shield regime for entities that self-certify.

Protection

Japan's final step in reaching data protection equivalence with the EU was the adoption of Supplementary Rules applicable to data transferred from the EU to Japan. The Supplemental Rules filled gaps between existing Japanese data privacy regulations, the 2003 Act on the Protection of Personal Information (APPI) and 2015 APPI amendments, and the GDPR. These Supplementary Rules apply to Japanese companies importing data from the EU and strengthen the protection of sensitive data, the rights of data subjects and the circumstances in which Japanese entities can further transfer EU data outside the country. The Supplementary Rules embrace principles at the heart of the GDPR such as data protection by design and by default, minimization of data collection and processing, and transparency regarding data use. In addition, the Japanese government indicated to the European Commission that Japanese public authorities would use personal data only as necessary and proportionate for criminal law enforcement and national security purposes.

Enforcement

An independent Japanese supervisory authority called the Personal Information Protection Commission (PPC) established by the amended APPI will be responsible for oversight and enforcement of the new Supplementary Rules. The PPC has authority to investigate improper use of data and issue binding decisions. In addition, the Supplementary Rules provide aggrieved EU data subjects with judicial and administrative recourse, which is similar to remedies available under the GDPR.

Key Takeaways

The mutual adequacy decisions create the world's largest area of free data flow. Of the decision on Japan, European Commissioner for Justice, Consumer and Gender Equality Vera Jourová remarked on its widespread impact, saying "Europeans' data will benefit from high privacy standards when their data is transferred to Japan. Our companies will also benefit from a privileged access to a 127 million consumers' market. Investing in privacy pays off; this arrangement will serve as an example for future partnerships in this key area and help setting global standards."

Return to Table of Contents

Illinois Supreme Court Holds That Biometric Privacy Law Does Not Require Actual Harm for Private Suits

The Illinois Supreme Court ruled that an Illinois biometric privacy law does not require individuals to show they suffered harm other than a violation of the law in order to bring suit. As a result, entities are at a greater risk of liability for failure to follow legally required procedures for handling biometric information collected or stored in Illinois.

Background

The Illinois Biometric Privacy Act (BIPA) is a uniquely expansive state law that imposes requirements on businesses that collect or otherwise obtain biometric information, including

[9] See here for an explanation of the process.

fingerprints, retina scans and facial geometry scans (which could include identifying individuals through photographs).[10] Among other requirements, businesses must receive written consent from individuals before obtaining their biometric data, and they must disclose their policies for usage and retention. Though Illinois was the first state to pass a law specifically regulating biometric data usage, other states are currently considering the issue, and Washington and Texas have already passed similar legislation. BIPA, however, is currently the only state law that allows private individuals to bring suit and recover damages for violations. For negligent violations, individuals can recover the greater of $1,000 or their actual losses. For reckless violations, the baseline award increases to $5,000.

In this class action, *Rosenbach v. Six Flags Entertainment Corp*., plaintiff Stacy Rosenbach argued that Six Flags violated BIPA when it required her son to scan his fingerprint in order to use a season pass. Rosenbach alleged that Six flags never informed her about the fingerprint requirement when she bought the pass, and they never provided a policy detailing how they would use or store the information. She did not claim that these violations of the law caused her any additional harm, financial or otherwise. BIPA allows "aggrieved" individuals to bring suit when an entity violates the requirements for handling their biometric data, and the parties disputed who qualifies as "aggrieved."

The Decision

On January 25, 2019, the Illinois Supreme Court held that private individuals may bring suit even if the only harm was a violation of their legal rights.[11] The court decided that anyone whose rights under BIPA were violated qualifies as "aggrieved," and rejected the argument that the violation needs to cause some type of additional harm. Since the Illinois legislature did not define "aggrieved," the court reasoned that the word should have its ordinary meaning, which has traditionally included the denial of a legal right. By passing BIPA, the Illinois legislature decided that individuals have rights of privacy and control over their biometric data. Thus, when an individual's BIPA rights are violated, they are "aggrieved" within that word's ordinary meaning.

The *Six Flags* decision clarifies who is allowed to bring a lawsuit for violations of BIPA. As other states pass similar laws in order to fill the federal void, they may decide to clearly resolve the issue in the text of their laws.[12]

Unresolved Issues

This decision leaves other important questions unresolved. In particular, courts have grappled with the question of which types of injuries are sufficiently "concrete" to give individuals constitutional standing to bring suit in federal court. In a recent ruling from a U.S. District Court in Illinois, the court emphasized that a technical violation of BIPA would not always be enough.[13] There, the court dealt with a challenge to the "face grouping" feature in Google Photos, which automatically scans photos to create face templates for different individuals. The court held that neither the retention nor the collection of face templates without authorization was a concrete injury. The court emphasized that, even assuming that users did not know Google was obtaining biometric data from their photos, there was no evidence that this practice created a substantial risk of harm because Google had not leaked or disclosed this information to third parties.

Other courts have come to different conclusions. Last year, a U.S. District Court in California held that Facebook users had standing to challenge Facebook's facial recognition feature, even though the only harm they alleged was a violation of their rights under BIPA.[14] The court relied on the Illinois legislature's finding that since biometric information cannot be changed, it presents heightened risks associated with identity theft. These divergent outcomes illustrate the range of approaches courts are taking in suits addressing technological harms. Some courts defer to legislative attempts at addressing perceived risks, while others require parties to show harms that can be analogized to traditional injuries.

For businesses that find themselves on the receiving end of a lawsuit under BIPA, there are other lines of defense that have not yet been resolved by courts. Some businesses may argue that individuals have effectively consented to the use of their data by

[10] The text of the BIPA can be found here.

[11] The decision is available online here.

[12] Federal agencies such as the FTC may be increasingly focused on instances of actual consumer harm, discussed here.

[13] The decision is available online here.

[14] The decision is available online here.

taking actions such as placing their hand on a fingerprint scanner. As a result, they may not have suffered an injury sufficient for constitutional standing. In the case of facial recognition, however, courts have been skeptical of this argument. Individuals may not know that by uploading a photo, they are subjecting it to facial geometry analysis.

Key Takeaways

Under Illinois law, failing to follow proper procedures for handling biometric information can expose businesses to liability, regardless of whether anyone is directly harmed in the process. As other states pass similar laws, this may vary on a state-by-state basis. Furthermore, courts remain divided on whether a violation of BIPA necessarily causes a concrete injury that confers constitutional standing.

In light of the emerging patchwork of state laws, businesses should undertake a careful state-by-state analysis before embarking on a biometric data collection effort. For example, under Texas law, voiceprint data used by financial institutions is not subject to the state's biometric identifier law, whereas in Washington, certain financial institutions are entirely exempt from any of the state's biometric data restrictions. These variances could create enough operational difficulty and expense that using nonbiometric alternatives may be the best option for many businesses.

BIPA Compliance Practice Pointers

When businesses use biometric data in Illinois, they should ensure that their practices comply with BIPA. As of now, BIPA applies to retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry. Many businesses use systems requiring employees to scan their fingerprints, and the law may also cover less obvious technologies. Past cases have challenged features such as photo-tagging in social media applications and video game avatars based on user face scans. Note, however, that BIPA removes certain types of data from its reach, including "information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment or operations under [HIPAA]." As a result, businesses should carefully consider each exception to determine their obligations.

Additionally, businesses should evaluate their business needs *before* collecting data. Businesses can reduce long-term compliance costs by taking the following considerations into account:

1. **Duration.** At most, an entity can retain information for the lesser of: (i) fulfillment of the purpose or (ii) three years after last contact with the data subject, whichever comes first. Thus, a narrow purpose may limit an entity's ability to retain useful biometric information for the needed duration.
2. **Scope.** If the scope of the purpose is too narrow at the outset for a later use, the business must obtain additional consent prior to undertaking that use, resulting in unnecessary delay and expense.
3. **Transferability.** Unless disclosure is required by law, covered entities are prohibited from sharing biometric information with a third party without the individual's prior consent, including with vendors and service providers.

Return to Table of Contents

European Data Authorities Release Annual Report Expressing Concerns With Privacy Shield

The European Data Protection Board has released a report on the EU-U.S. Privacy Shield framework, in which it expressed a number of concerns with the program.

On January 22, 2019, the European Data Protection Board (EDPB) released its second annual report on the effectiveness of the EU-U.S. Privacy Shield.[15] The report expressed a wide range of concerns over the program's effectiveness. The EDPB is an independent body and its report is not binding on European authorities, but its views historically have carried a good deal of weight with regulators.

Background on Privacy Shield

In 2016, the United States and the European Commission adopted the EU-U.S. Privacy Shield, a self-certification framework designed to enable companies to transfer personal data from the EU and the three European Economic Area member

[15] The report is available here.

states — Norway, Liechtenstein and Iceland — to the U.S. Under the EU Data Protection Directive, EU citizens' personal data can be transferred only to countries with "adequate" data protection laws in place. The U.S. does not meet this standard. However, under the Privacy Shield, companies that self-certify their adherence to seven broad data privacy principles may transfer personal data outside of the EU to the U.S.

Praise and Criticism

In its report, the EDPB praised a number of U.S. efforts to implement the Privacy Shield, including:

- efforts to adapt the initial certification process to minimize the inconsistency between when a company announces its Privacy Shield certification and when the Department of Commerce updates the Privacy Shield certification list on its website;
- enforcement actions taken by the Department of Commerce and the FTC related to Privacy Shield compliance; and
- Department of Commerce guidance to EU individuals on exercising their rights under the Privacy Shield and for U.S. companies on their Privacy Shield obligations.

On the other hand, the report also expressed a number of concerns related to how the Privacy Shield has been implemented to date, including:

- a lack of actual verification of companies' compliance with the Privacy Shield requirements;
- a lack of oversight of companies' compliance with "onward transfer" obligations related to the further transfer of EU-sourced personal information after it has been delivered to the U.S.;
- delays in updating the Department of Commerce's Privacy Shield list with respect to companies re-certifying their Privacy Shield compliance;
- ongoing uncertainty on how the Privacy Shield applies to human resources data; and
- a lack of certainty as to the independence and effectiveness of the ombudsperson, who is supposed to facilitate requests from EU individuals relating to national security access to data transmitted from the EU to the U.S., due in part to the fact that the position lacks a permanent appointment.

Key Takeaways

Many of the issues cited in the EDPB's report have been raised before (including in the board's first annual report) and remain unresolved. As the various legal challenges to the Privacy Shield work their way through EU courts, it is likely that many of these issues will be raised in those proceedings. Whether EU data protection authorities or courts will seek to revise, or even reject, the Privacy Shield unless they are addressed remains to be seen. Until then, the Privacy Shield remains in place and has been an important tool for enabling data transfers from the EU to the U.S.

Return to Table of Contents

Privacy & Cybersecurity Update
Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000